COE Security Update

7 September 2001

Mr. Matt O’Brien
Science Applications International Corp.
(703) 676-5032
obrienma@saic.com

Mr. Quang Nguyen
COE Security Engineer
Defense Information Systems Agency
(703) 735-8758

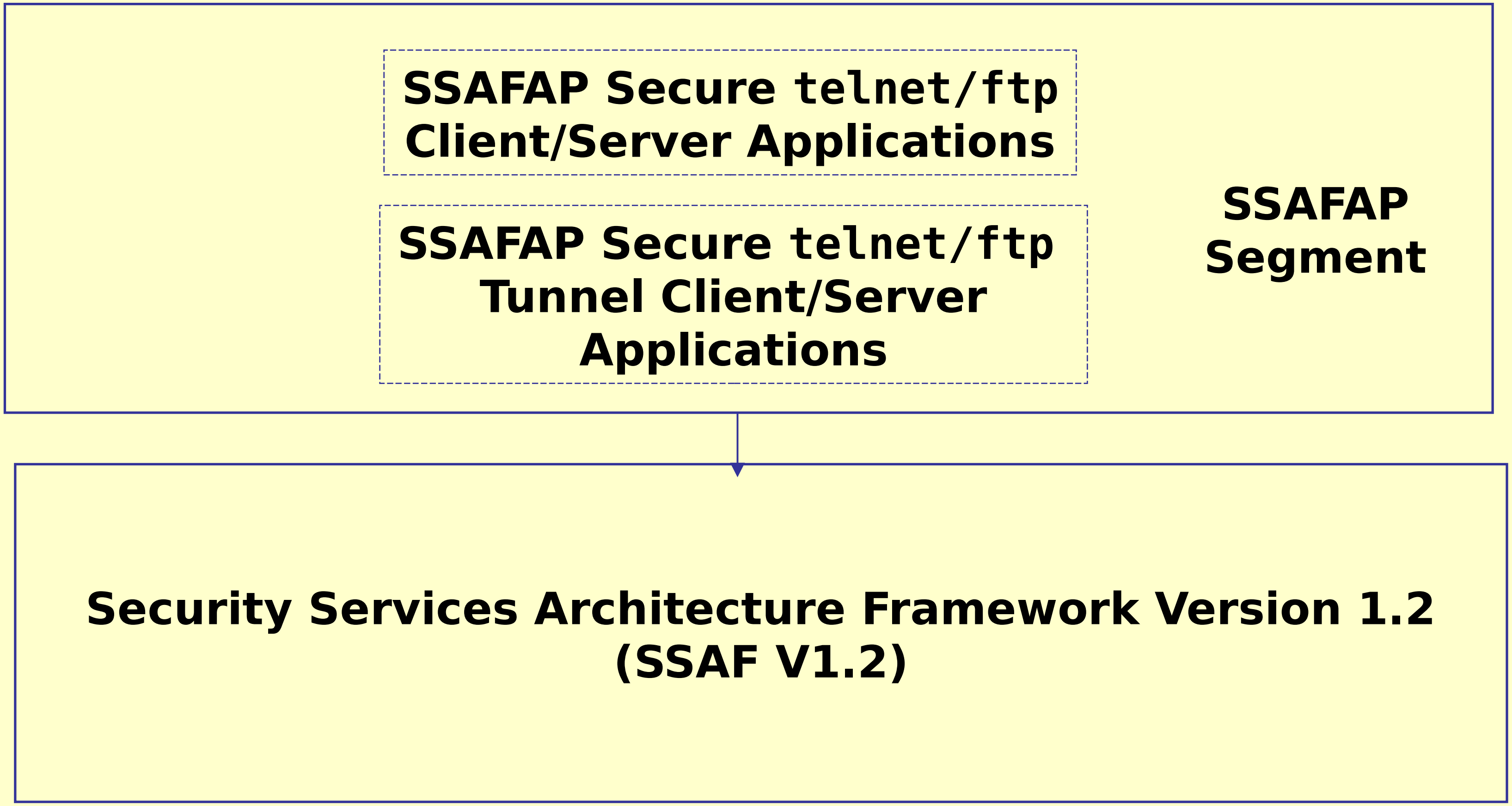
Agenda

- □ **Secure `telnet` and `ftp` Application**
- □ **UNIX Security Lockdown**
- □ **Windows Security Lockdown**

Secure telnet and ftp Application

- The SSAF Application (SSAFAP) segment (delivered 8/31) provides the capability to secure the standard `telnet` and `ftp` services (that send an unencrypted password across the wire)
- SSAFAP uses the encryption services of the Security Services Architecture Framework V1.2 (SSAF V1.2), and therefore requires the installation of the SSAF V1.2 segments.
- The SSAFAP segment installs on the Windows NT 4.0 & 2000, Solaris 7/8, and HP-UX 11 platforms.

SSAFAP Architecture



SSAFAP Secure telnet/ftp Client/Server Applications

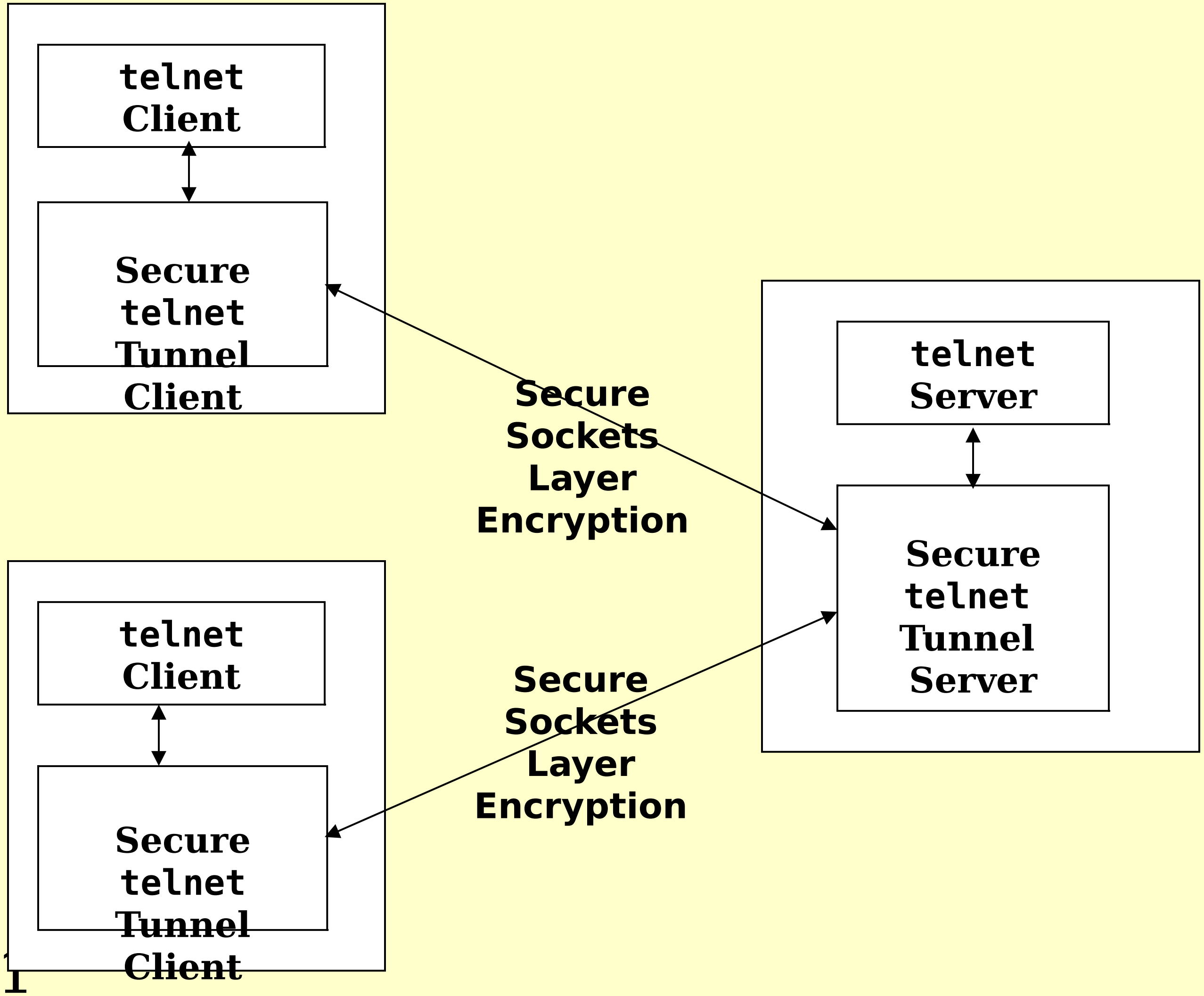
SSAFAP Secure telnet/ftp Tunnel Client/Server Applications

SSAFAP Segment

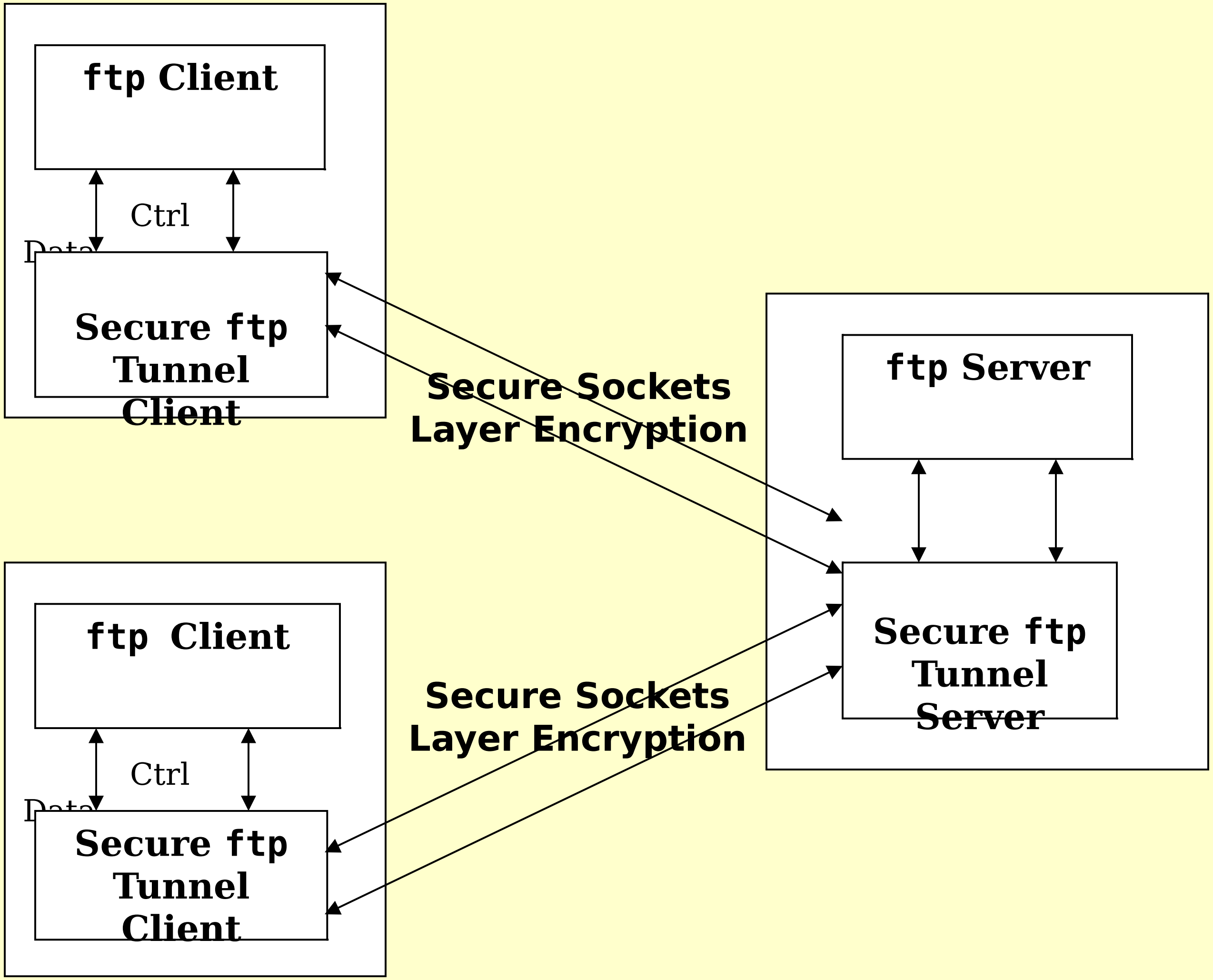
Security Services Architecture Framework Version 1.2 (SSAF V1.2)

9/7/01

Securing telnet: The Concept


telnet Client
Secure telnet Tunnel Client
Secure Sockets Layer Encryption
telnet Server
Secure telnet Tunnel Server
telnet Client
Secure telnet Tunnel Client
Secure Sockets Layer Encryption

Securing ftp: The Concept



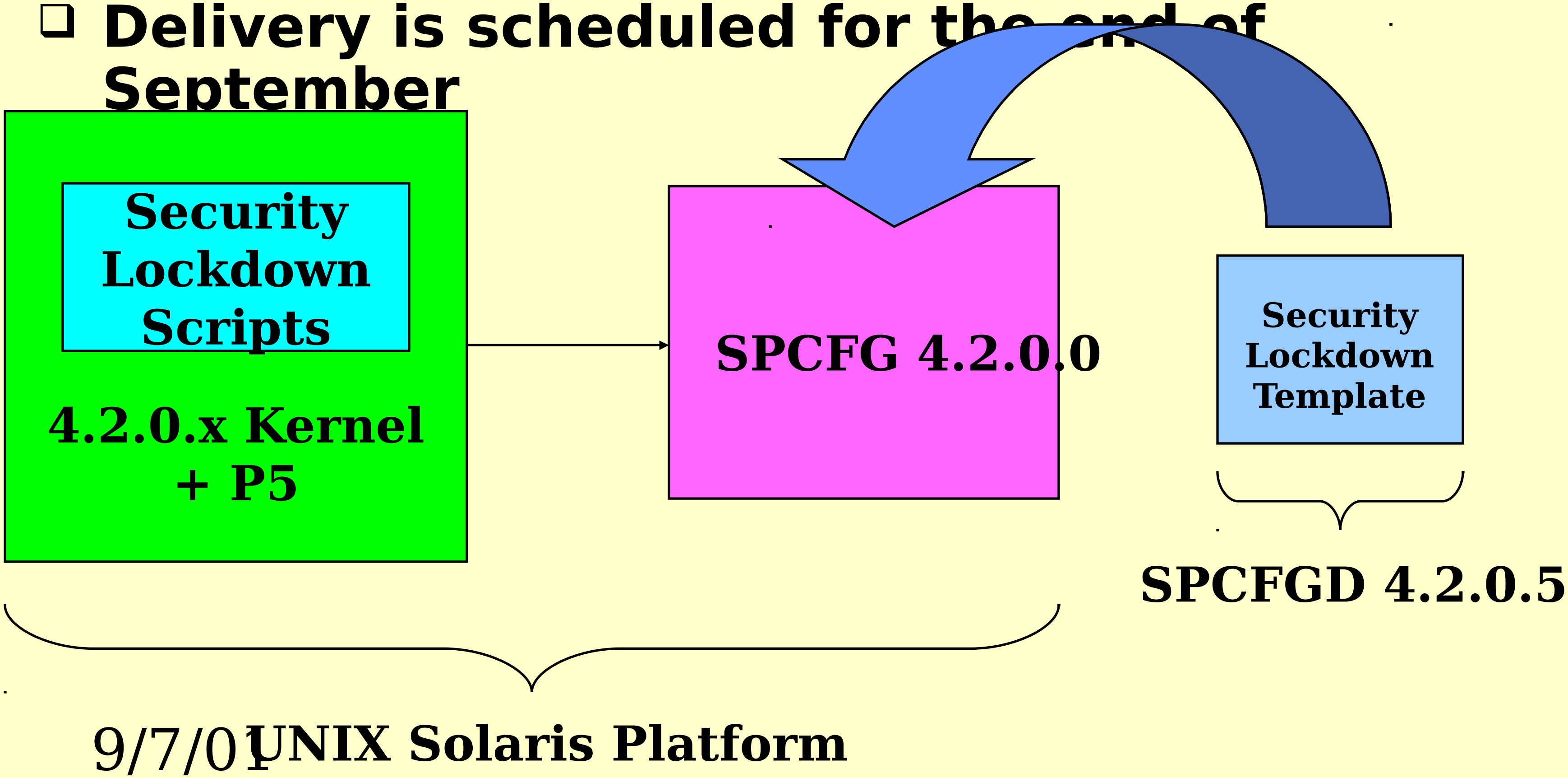
9/7/01

SSAFAP CONOPS Issue

- **SSAFAP requires that the telnet and ftp services be re-enabled on the server host.**
- **SSAFAP does not replace the telnet application nor does it implement the telnet protocol, but rather redirects the data stream from an existing telnet application into the SSAFAP Secure Tunnel.**
- **The non-secure versions of telnet and ftp are therefore also available to users**
- **Should SSAFAP implement a technical solution to ensure only secure telnet**

UNIX Security Lockdown

- The SPCFGD 4.2.0.5 security lockdown template will re-apply the P5 security lockdown
- Delivery is scheduled for the end of September



Windows Security Lockdown

- □ **Windows security templates (for P4 and earlier) must be applied according to the build sequence diagrams**

- □ **These templates must be applied before segment installation; otherwise, they will overwrite segment permissions due to inheritance**

- □ **The P5 release (4.5.0.0) of the Windows security templates will support re-applying the templates after segment installation**

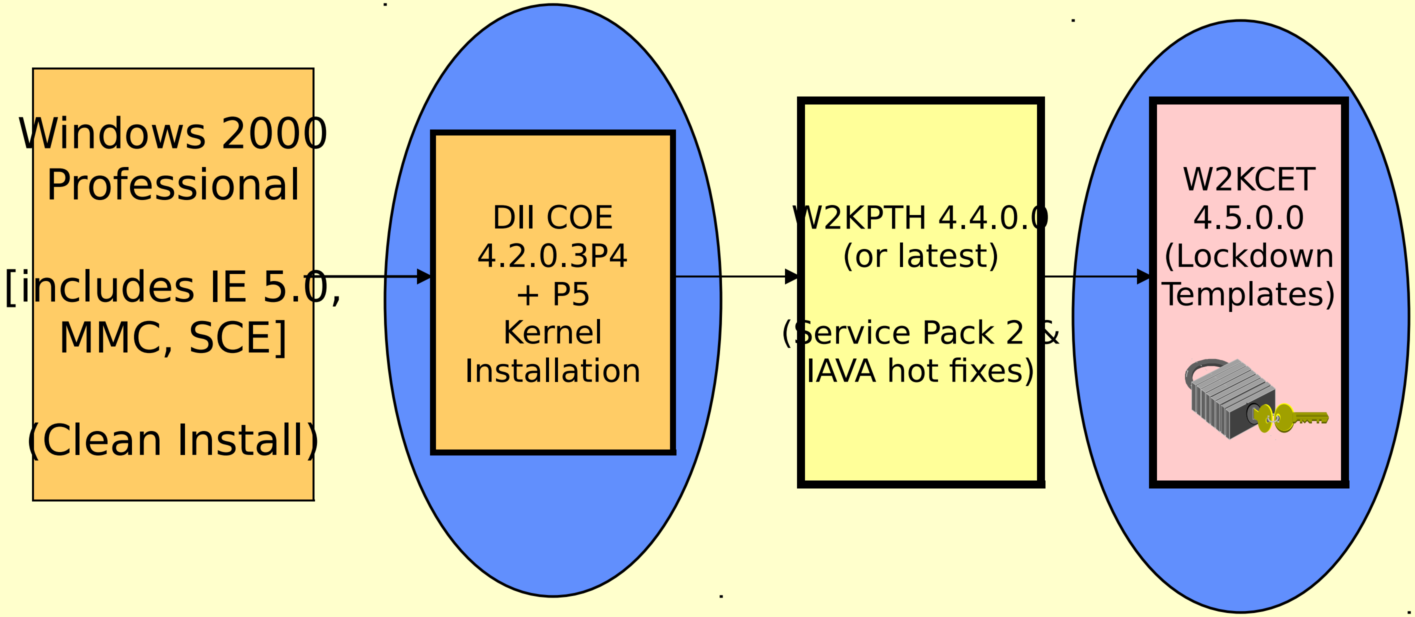
- □ **A future release will include both pre-**

Windows Security Templates: Usage

Windows 2000 Build Sequence

Partial security lockdown is performed during kernel installation

Security lockdown is completed with template installation



Windows 2000 Professional

[includes IE 5.0, MMC, SCE]

(Clean Install)

DII COE 4.2.0.3P4 + P5 Kernel Installation

W2KPTH 4.4.0.0 (or latest)

(Service Pack 2 & IAVA hot fixes)

W2KCET 4.5.0.0 (Lockdown Templates)

9/7/01

Windows Security Templates: Schedule

- ❑ **The W2KCET 4.5.0.0 segment for Win2K Pro will be delivered at the end of September**
- ❑ **The MSSCET 4.5.0.0 segment for NT workstation, server and PDC will be delivered end of October**
- ❑ **A future release of W2KCET will provide security templates for server and Domain Controller**

9/7/01

Windows Security Templates: Recommendations

- For P4 and earlier, use the appropriate MSSCET and W2KCET segments
- For P5 NT (workstation, server and PDC), the kernel security lockdown provides adequate security until MSSCET 4.5.0.0 segment is available end of October

Windows Security Templates: Recommendations (2)

❑ For P5 Win2K Pro, an engineering drop of W2KCET 4.5.0.0 will be available end of Sep (formal delivery to DISA CM at same time)

❑ For P5 Win2K Server and Domain Controller, COE Security team discourages operational use until security templates are delivered and Active